Aiello 1999-0053

IN THE CLAIMS:

Claims 1 – 35 (delete).

36. (Currently Amended) ~~The method of claim 35 further of:~~ A method of
employing a user's broadband telephony interface (BTI), executed in said BTI in
communication with a network, comprising the steps of:

sending a request to a provisioning server;

receiving a key of said provisioning server and information that authenticates said
provisioning server;

generating a random key K and its complement, a random session key SK and its
complement, and a random audio channel key AK and its complement, where a
complement of a key J is a key that decrypts ~~messages~~ message encrypted with said
key J;

sending to said provisioning server information that includes said complement of
said K encrypted with said key of said provisioning server, and a tuple encrypted with
said K, which tuple includes said complement of said SK, and said complement of said
AK;

receiving an acknowledgement from said provisioning server;

establishing a voice connection between said user and said network;

receiving from said provisioning server a request over said voice connection,
encrypted with said complement of said key AK

relaying said request to said user;

receiving responsive information from said user;

forwarding said responsive information to said provisioning server, encrypted
with said key AK;

generating a public/private key pair; and

sending the generated public key to said provisioning server, encrypted with said
key SK.

37. (Previously Presented) The method of claim 36 further comprising the step
of receiving an acknowledgement message from said provisioning server, in response to

2

Aiello 1999-0053

said sending of the generated public key, which acknowledgement message is encrypted with said complement of said key SK.

Claims 38 – 39 (delete).

3